Security Awareness Video Transcript

You are the Target/Don’t Be the Weakest Link

The content of this video is for informational purposes only. Agencies may have additional policies or procedures in place.

Each day thousands of security breaches take place in the US alone. Many of these could have been stopped with some basic security knowledge.

What is Security Awareness?

Security Awareness knowledge allows you to protect an organization’s assets and information. In this presentation we are going to teach you how to better protect information, passwords, email, and physical assets.

Information Protection

Information is the livelihood of all organizations. Whether you run a lemon-aid stand or a Fortune 500 business, the information that you own must be protected.

Special data protections are also required by laws and regulations to protect their data.

We can classify data two ways :
Sensitive: This data must be protected and should only be shared with authorized people. Even if someone works with you it does not mean they should have access to this information, and
Non-Sensitive: This data is ok to share with all users.

If you are not sure what type of information you have you should treat it as sensitive data.

Remember that data needs to be protected in all formats.

- When copying data to a thumb drive or other physical media you need to ensure that the same level of protection is applied,
- Proper disposal of data is also important. You must shred sensitive data when disposing of it,
- When discussing sensitive information make sure other individuals are not listening in to your conversation, and
- When leaving a meeting space ensure whiteboards are clean and that all sensitive information is taken with you.

Password Protection

Passwords are still the primary defense in most information systems. By following a few simple rules you can make your passwords stronger.

- Remember that all passwords are important. If the system requires a password then there is some type of sensitive information is available on that system.
- Use different passwords for different accounts and avoid using proper names or common words.
- It is important never to share a password or write down a password in a place where it can be found.
- If you need to use a large number of passwords, then special applications are available to help you keep them secure without memorizing each one.

Creating a Good Password

Let's take a look at how to take a simple word and create a good password.

- Start with the word **Frankfort** and spell it backwards, **trofknarf**, you can see now that this would be a more difficult password to guess.
- Next, add some substitution for certain letters. We can replace the '**o**' with a '**0**' and the '**a**' with an '**@**'symbol - **tr0fkn@rf.**
- Finally capitalize a few letters, such as the'**T**' and the '**N**' – **Tr0fkN@rf**.

We now have a password that is difficult to guess and would be harder for an attacker to break.

Email and Phishing

Email is the most commonly used method of business communication today. Here are a few simple tips for safe email use.

- Never open an attachment that you are not expecting. Even if you know the sender, the attachment may not be safe.
- Always verify your addresses. Often we will use the auto-fill feature of email clients. This can cause sensitive information to be sent to the wrong people.
- You should also use the BCC field when sending to a large group of people.
- Phishing is a significant security risk associated with email and social media. In a phishing attack a hacker tries to fool you into providing sensitive information. There a few simple things we can look for to stop a phishing attack.

    1. Read the message carefully. If it appears to be generic or refers to something you never did it is probably a fake email.
    2. Also check the actual URL of any link in the message. If it doesn't match the text or if it doesn't point to a legitimate site, do not click on the link.
    3. If you aren't sure whether an email is legitimate or not, it is best to assume it is not, and do not click the links or provide sensitive information.

Physical Protection

Not all security involves computers.

There are some basic guidelines for physical security, too.

- Always secure sensitive information when you leave the office.
- If a location is supposed to be locked do your job to ensure it stays locked.
- Security badges are useful but they must be used correctly. Remember they do more than just open the door to your building- they also record information about who has entered the building. Do not share your badge or tailgate on someone else's.
- When you have a mobile device with sensitive information on it you should take extra care to ensure it does not fall into the wrong hands.

Conclusion

Congratulations, you can now better protect the information and assets of your organization. You can be a strong link.

Thank you for completing the security awareness training. Please complete the acknowledgement form. You will need to sign and date the form and give it to you supervisor.